Amendments

Please amend the claims as follows:

Claim 1. (original) A method for preventing intrusion in a communications network having a plurality of nodes, comprising the steps of:

initiating a request for network services by a source node;

constructing a transformed packet header and transmitting a synchronization packet with the transformed packet header to a destination node;

authenticating the received packet by examination of the transformed packet header;

releasing the authenticated packet to the destination node; and

reforming the transformed packet header at the destination node.

Claim 2. (original) The method for preventing intrusion in a communications network of claim 1 further comprising the step of transmitting an acknowledgement response with a transformed packet header to the source node.

Claim 3. (original) The method for preventing intrusion in a communications network of claim 1 wherein the request for network services is a request for a session connection with the destination node.

Claim 4. (original) The method for preventing intrusion in a communications network of claim 1 further comprising the step of authenticating a source identification by comparing a previously stored value with the source identification value determined for the source node.

Claim 5. (original) The method for preventing intrusion in a communications network of claim 4 wherein the previously stored value and the determined source identification value are based on a hardware address of the source node and an associated user identification.

Claim 6. (original) The method for preventing intrusion in a communications network of claim 4 wherein the request for network services is terminated if the determined source identification value does not match the previously stored value.

Claim 7. (original) The method for preventing intrusion in a communications network of claim 6 further comprising the step of reporting the termination of the request for network services in a message to a network administrator and storing the message in an unauthorized event database.

Claim 8. (original) The method for preventing intrusion in a communications network of claim 1 wherein the step of constructing a transformed packet header comprises the steps of:

selecting a key index value from a first array of key index values;

applying the selected first array key index value to transform a user identification;

appending the first array key index value to the transformed user identification;

selecting a key index value from a second array of index values;

applying the second array key index value to the transformed user identification and appended first array key index value to form a first packet header field; and

storing the first packet header field in a transmit buffer.

Claim 9. (original) The method for preventing intrusion in a communications network of claim 8 wherein the step-of constructing a transformed packet header further comprises the steps of:

appending the second array key index value to a determined source identification value to form a resulting source identification value;

applying a transformation routine to the resulting source identification value to form a second packet header field; and

storing the second packet header field in the transmit buffer.

Claim 10. (original) The method for preventing intrusion in a communications network of claim 1 further comprising the steps of:

inspecting each received packet to determine a corresponding transport protocol;

inspecting each received packet matching a selected protocol type to determine if the received packet is a synchronization packet;

retaining the received packet for further processing if the received packet is a synchronization packet.

Claim 11. (original) The method for preventing intrusion in a communications network of claim 10 further comprising the step of releasing the received packet if it does not match a selected protocol type.

Claim 12. (original) The method for preventing intrusion in a communications network of claim 10 further comprising the step of releasing the received packet if it is not a synchronization packet.

Claim 13. (original) The method for preventing intrusion in a communications network of claim 1 wherein the step of authenticating the received packet comprises the steps of:

determining if the received packet originated from a trusted source node; and

executing an exception module if the received packet originated from an untrusted source node.

Claim 14. (original) The method for preventing intrusion in a communications network of claim 1 wherein the step of authenticating the received packet comprises the steps of: determining if the received packet originated from a trusted source node; examining the packet header of the received packet to determine if the packet header has been transformed by the

source node; extracting a determined source identification value and an associated source user identification from the transformed packet header; and inspecting the packet header to determine if an access policy is specified for the source node.

Claims 15-32 (canceled)

Claim 33. (original) A method for providing trusted communications between a source device and a destination device in a communications network, comprising the steps of: initiating a request for a communications session at the source device; constructing a transformed packet header and transmitting a synchronization packet including the transformed packet header to the destination device; receiving the synchronization packet at the destination device; reforming the transformed packet header at the destination device; and constructing a transformed packet header and transmitting an acknowledgement response including the transformed packet header to the source device.

Claims 34-63 (canceled)

Claim 64. (original) An appliance for providing trusted communications in a communications network, comprising:

a component for receiving a plurality of packets including transformed packet headers from a client device;

a component for authenticating the plurality of received packets by examination of the transformed packet headers; and

a component for releasing authenticated packets to another client device.

Claims 65-66. (canceled)

67. The appliance for providing trusted communications of claim 64 further comprising:

a component for inspecting each received packet to determine a corresponding transport protocol; and

a component for determining if each received packet is a synchronization packet.

Claim 68. (original) The appliance for providing trusted communications of claim 64 wherein the authentication component comprises

a component for determining if the received packet originated from a trusted client device; and

a component for executing an exception routine if the received packet originated from an untrusted client device.

Claim 69. (original) The appliance for providing trusted communications of claim 64 further comprising:

a component for determining if the received packet originated from a trusted client device;

a component for determining if the packet header has been transformed by the client device;

a component for extracting a determined client device identification value and an associated user identification from the transformed packet header; and

a component for inspecting the packet header to determine if an access policy is specified for the client device.

Claims 70-77. (canceled)

Claim 78. (original) A client device for providing trusted communications in a communications network, comprising:

a component for initiating a request for a communications session;

a component for constructing a transformed packet header for transmission in a synchronization packet to a network device;

a component for receiving a plurality of packets including transformed packet headers from a network device;

a component for reforming transformed packet headers received from a network device; and

a component for constructing a transformed packet header for transmission with an acknowledgement response to the network device.

Claims 79-117 (canceled)